Algebraic Structures- Solutions of Homework 3

written by Motke Porat

November 2017

1 Question 1.

1.1 (c):

Clearly $\{x.gx, g^2x, ...\} = \{x, gx, ..., g^{p-1}x\}$. Moreover,

- if $g^jx = x$ for some $1 < j < p$, then j and p are coprime and there exist $n, m \in \mathbb{Z}$ such that $nj + mp = 1$, so

$$gx = g^{nj+mp}x = x$$

  and we get $|\{x, gx, ..., g^{p-1}x\}| = |\{x\}| = 1$.

- if $g^jx \neq x$ for all $1 < j < p$, then $|\{x, gx, ..., g^{p-1}x\}| = p$.

1.2 (d):

X is the disjoint union of all orbits of $\langle g \rangle$,

$$X = \bigcup_i \{x_i, gx_i, g^2x_i, ...\}$$

and from part (c) we know that each orbit $\{x_i, gx_i, g^2x_i, ...\}$ is of length 1 or p. If all the orbits were of length p then $p \mid |X| = n$ which is a contradiction to the assumption that $gcd(p, n) = 1$, therefore there is an orbit of length 1, i.e., there exists $x_i \in X$ for which $gx_i = x_i$.

2 Question 2.

2.1 (b):

The rule $(h, g) \to gh^{-1}$ defines a group action:

- $(e, g) \to ge^{-1} = g$ for any $g \in G$,
- $(h_1h_2, g) \to g(h_1h_2)^{-1} = g(h_2^{-1}h_1^{-1}) = (h_1, gh_2^{-1}) = (h_1, (h_2, g))$ for every $h_1, h_2 \in H$,.

The rule $(h, g) \to gh$ is not a group action, as

$$(h_1h_2, g) = gh_1h_2 \neq gh_2h_1 = (h_1, (h_2, g))$$

and it is enough to take $g = e$ and h_1, h_2 which not commute.

2.2 (c):

Take the following mapping from the set of all right cosets of H to the set of all left cosets of H:

$$\phi : \{aH : a \in G\} \to \{Ha : a \in G\}, \quad \phi(aH) = Ha^{-1}.$$

Then-

- The mapping ϕ is well defined, as if $a_1H = a_2H$ then $a_1^{-1}a_2 \in H$ and hence
$$\phi(a_1H) = Ha_1^{-1} = Ha_1^{-1}a_2a_2^{-1} = Ha_2^{-1} = \phi(a_2H).$$
- If $\phi(aH) = \phi(bH)$, then $Ha^{-1} = Hb^{-1}$ which means that there exist $h_1, h_2 \in h$ such that $h_1a^{-1} = h_2b^{-1}$ and thus $a^{-1}b \in H$. Therefore
$$bH = a(a^{-1}b)H = aH$$
and ϕ is $1-1$.
- For every right coset Hb of H, we have
$$\phi(b^{-1}H) = H(b^{-1})^{-1} = Hb$$
so ϕ is onto the set of all right cosets of H.

Notice that the mapping $\phi : aH \to Ha$ is not a good one for us, as it is not well defined: let $G = S_3$ and $H = \{(1), (12)\}$, then it is easy to check that

$$(1,3)H = \{(1,3), (1,3,2)\} = (1,3,2)H$$

but

$$\phi((1,3)H) = H(1,3) = \{(1,3), (1,2,3)\} \neq \{(1,3,2), (2,3)\} = H(1,3,2) = \phi((1,3,2)H).$$

3 Question 3.

3.1 (a): No, here is a counterexample:

Let $G = A_4, n = |A_4| = 4!/2 = 12$ and there is no a subgroup of A_4 of order 6: the group A_4 consists of 12 permutations:

- the identity (1),
- 3 products of 2 cycles of length 2:
$$(1,2)(3,4), (1,3)(2,4), (1,4)(2,3)$$
- 8 cycles of length 3, separated into 4 pairs:
$$(1,2,4), (1,4,2), \quad (1,3,4), (1,4,3), \quad (1,2,3), (1,3,2), \quad (2,3,4), (2,4,3).$$

If H is a subgroup of A of length at least 6, then:

- H contains at least 2 cycles of length 3,

- if H contains 2 cycles of length 3 from 2 different pairs, then H has to be equal to A_4. For example, if $(1,2,3),(1,4,2) \in H$ then their inverses $(1,3,2),(1,2,4)$ belong to H and all the products

$$\begin{aligned}(1,2,3)(1,4,2) &= (2,3,4),\\ (1,4,2)(1,2,3) &= (1,4,3),\\ (1,3,2)(1,4,2) &= (1,3)(2,4)\end{aligned}$$

  belong to H and then $H = A_4$.

- if H contains a cycle of length 3 and a product of two cycles of length 2, then it contains 2 cycles of length 3 that correspond to 2 different pairs, and hence $H = A_4$. For example, if $(1,2,3) \in H$ and $(1,3)(2,4) \in H$, then also $(1,2,3)(1,3)(2,4) = (1,4,2) \in H$.

Therefore, if h is a subgroup with at least 6 elements, then it must be equal to A_4, so A_4 does not have any subgroups of order 6.

3.2 (c):

In question 1 of homework 2 you showed that $(\mathbb{Z}_n^\times, \cdot, \overline{1})$ is a group of order $\varphi(n)$, where $\mathbb{Z}_n^\times$ is the subset of $\mathbb{Z}_n$ consists of all the invertible elements. If

$$gcd(a,n) = 1$$

then a is an invertible element in $\mathbb{Z}_n$ and therefore $a \in \mathbb{Z}_n^\times$. A corollary of the Lagrange theorem tells us that $x^{|G|} = 1$ for every $x \in G$. In our case, we get that $|\mathbb{Z}_n^\times| = \varphi(n)$ and hence

$$a^{\varphi(n)} = \overline{1} \Longrightarrow a^{\varphi(n)} = 1(\mod n).$$

4 Question 4.

4.1 (b): No, here is a counterexample:

Let $G = A_4, H = \{(1),(1,2)(3,4),(1,3)(2,4),(1,4)(2,3)\}$ and $N = \{(1),(1,2)(3,4)\}$. It is easy to check that H is a subgroup of G, while $H \lhd G$ can be verified by the simple property that

$$\sigma^{-1}(i,j)(k,t)\sigma = (\sigma(i),\sigma(j))(\sigma(k),\sigma(t)) \in H$$

for every $\sigma \in A_4$. The fact that $N \lhd H$ follows as the index of H in G is equal to $|H|/|N| = 2$.

4.2 (c):

Let $H < G$ and $N := \cap_{g\in G} g^{-1}Hg$. Clearly N is a subgroup of G as the intersection of the subgroups $g^{-1}Hg$ for all $g \in G$. Moreover, for every $a, g \in G$ and $n \in N$, by the definition of N we know that

$$n \in (ga^{-1})^{-1}H(ga^{-1}) = ag^{-1}Hga^{-1} \Longrightarrow a^{-1}na \in g^{-1}Hg$$

and thus $a^{-1}na \in \cap_{g\in G} g^{-1}Hg = N$, so we have $N \lhd G$.

5 Question 7.

Let $\mathbb{F}$ be a field with q elements.

- How many invertible $n \times n$ matrices over $\mathbb{F}$ are there? In order to construct an invertible $n \times n$ matrix over $\mathbb{F}$, we have to choose the first column of the matrix to be any vector in $\mathbb{F}^n$ but zero, so we have $q^n - 1$ options; for choosing the second column we can choose any column in $\mathbb{F}^n$ except for products by scalar of the first column, so we have $q^n - q$ options;... In general, for choosing the k column we can choose any column in $\mathbb{F}^n$ except for any vector in the span of the first $k-1$ columns, so there are $q^n - q^k$ options. Therefore, we have exactly

$$(q^n - 1)(q^n - q)...(q^n - q^{n-1}) = \prod_{k=0}^{n-1}(q^n - q^k)$$

invertible $n \times n$ matrices over $\mathbb{F}$, i.e., $|GL_n(\mathbb{F})| = \prod_{k=0}^{n-1}(q^n - q^k)$.

- The group $SL_n(\mathbb{F})$ can be described also as the kernel of the determinant mapping $\det(\cdot) : GL_n(\mathbb{F}) \to \mathbb{F}^\times$ and as this mapping is onto $\mathbb{F}^\times$, we have

$$|SL_n(\mathbb{F})| = \frac{|GL_n(\mathbb{F})|}{|\mathbb{F}^\times|} = \frac{\prod_{k=0}^{n-1}(q^n - q^k)}{q-1} = q^{n-1}(q^n - 1)\prod_{k=1}^{n-2}(q^n - q^k).$$